

Cybersecurity Study Programs: What's in a Name?

Jan Vykopal

Masaryk University
Faculty of Informatics
Brno, Czech Republic
vykopal@fi.muni.cz

Michael Tuscano Lopez II

Ateneo de Manila University
Department of Information Systems and Computer Science
Quezon City, Philippines
michael.lopez@student.ateneo.edu

Valdemar Švábenský

Kyushu University
Faculty of Information Science and Electrical Engineering
Fukuoka, Japan
valdemar.research@gmail.com

Pavel Čeleda

Masaryk University
Faculty of Informatics
Brno, Czech Republic
celeda@fi.muni.cz

Abstract

Improving cybersecurity education has become a priority for many countries and organizations worldwide. Computing societies and professional associations have recognized cybersecurity as a distinctive computing discipline and created specialized cybersecurity curricular guidelines. Higher education institutions are introducing new cybersecurity programs, attracting students to this expanding field. In this paper, we examined 101 study programs across 24 countries. Based on their analysis, we argue that top-ranked universities have not yet fully implemented the guidelines and offer programs that have “cyber” in their name but lack some essential elements of a cybersecurity program. In particular, most programs do not sufficiently cover non-technical components, such as law, policies, or risk management. Also, most programs teach knowledge and skills but do not expose students to experiential learning outside the traditional classroom (such as internships) to develop their competencies. As a result, graduates of these programs may not meet employer expectations and may require additional training. To help program directors and educators improve their programs and courses, this paper offers examples of effective practices from cybersecurity programs around the world and our teaching practice.

CCS Concepts

• **Social and professional topics** → **Computing education; Computing education programs**; • **Security and privacy**;

Keywords

cyber security, curricular guidelines, CSEC2017, CC2020, higher education, university programs, global perspective

ACM Reference Format:

Jan Vykopal, Valdemar Švábenský, Michael Tuscano Lopez II, and Pavel Čeleda. 2025. Cybersecurity Study Programs: What's in a Name?. In *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE TS 2025)*, February 26–March 1, 2025, Pittsburgh, PA, USA, <https://doi.org/10.1145/3641554.3701976>.

1 (SIGCSE TS 2025), February 26–March 1, 2025, Pittsburgh, PA, USA. ACM, New York, NY, USA, 7 pages. <https://doi.org/10.1145/3641554.3701976>

1 Introduction

Due to the global prevalence of cyber crime and its impacts [9], cybersecurity is of utmost importance in a wide variety of sectors, from business through healthcare to national security. As a result, enhancing cybersecurity education is a strategic goal defined in the policies of numerous countries across the world [1], aiming to address the growing demand for cybersecurity professionals [27].

Higher education institutions have been responding to this demand by establishing cyber study programs to attract students to this field, which is expected to continue growing. Subsequently, educators have been sharing their insights and perspectives to encourage dialogue around cybersecurity curricula and facilitate their improvements. Particularly at computing education venues like SIGCSE, this topic has been of interest in recent years [2, 5, 11, 41].

1.1 Situating Cybersecurity Within Computing

Computing includes “computer science and related disciplines, such as computer engineering, information systems, information technology, software engineering, cybersecurity, and data science” [18]. Curricular efforts to define the content of computing degree programs date from at least the 1960s, and the evolution of cybersecurity coverage within these curricula is notable, as described by [38]. The influential 1968 ACM recommendations [3] do not mention the term “security” at all. Another seminal text from 1989 [15] makes only a brief reference to “secure computing”. Today, ACM/IEEE Computing Curricula 2020 (CC2020) [8] recognize cybersecurity as an essential component of educating computing professionals. Moreover, specialized cybersecurity curricular guidelines have emerged in recent years [20, 23], most notably:

- ACM/IEEE/AIS SIGSEC/IFIP JTF Cybersecurity Curricula – CSEC2017 [31] and its adaptation for community colleges, Cybersecurity Curricular Guidance – Cyber2yr2020 [30],
- NIST National Initiative for Cybersecurity Education – NICE (USA) [34],
- NCSE Cyber Security Body of Knowledge – CyBOK (UK) [33],
- ENISA European Cybersecurity Skills Framework – ECSF (EU) [32].

SIGCSE TS 2025, February 26–March 1, 2025, Pittsburgh, PA, USA

© 2025 Copyright held by the owner/author(s).

This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE TS 2025)*, February 26–March 1, 2025, Pittsburgh, PA, USA, <https://doi.org/10.1145/3641554.3701976>.

Cybersecurity is a multidisciplinary field encompassing various computing domains, including secure programming, network defense, and operating system administration, along with non-technical aspects [38]. To become proficient in these subjects, students require theoretical foundations and practical experience with relevant tools and processes [31]. Delivering this experience necessitates realistic learning environments and current, relevant tasks. However, since cybersecurity is an ever-evolving field, tools and procedures that worked yesterday might be obsolete today. Fortunately, there are modern opportunities for students to enhance their cybersecurity knowledge and skills [11, 39, 42].

1.2 Current Motivating Context

While understanding cybersecurity concepts is an essential starting point for prospective cybersecurity experts, it alone is not fully sufficient [20]. Cybersecurity professionals also require hands-on experience with applying cybersecurity skills in practical contexts. As early as 2014, it was observed that many university graduates were unprepared for cybersecurity roles due to a lack of industry-required practical skills [10]. This gap between academic preparation and workplace requirements has been pointed out again in the CSEC2017 guidelines [31]. Yet, these concerns still remain relevant in 2024: Crabb et al. [11] observed that curricular recommendations for universities emphasize knowledge acquisition and understanding of concepts, whereas the industry expects job candidates with higher-level application skills. Lastly, Sui [27] raises similar concerns about “noncompliance with international standards”.

1.3 Goals and Scope of This Paper

This paper examines *whether cybersecurity study programs offered by leading universities incorporate the elements recommended in curricular guidelines and valued by employers* (see Figure 1). We analyzed cybersecurity study programs offered by 101 universities and educational institutions globally, focusing on descriptions of these programs and offered courses. Therefore, we aim to address overarching issues beyond individual course details. Specifically, we closely inspected *i*) the inclusion of non-technical aspects, such as law, policy, human factors, ethics, and risk management, and *ii*) the integration of experiential learning within these study programs.

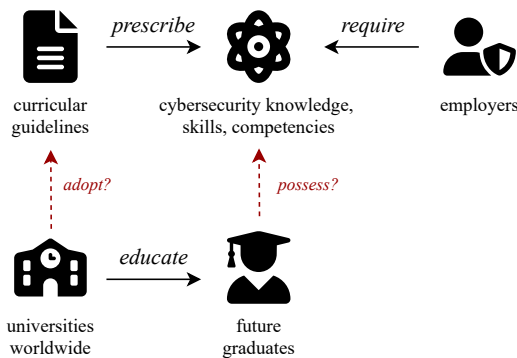


Figure 1: Cybersecurity curricular guidelines define knowledge, skills, and competencies required by employers. But do universities adopt these guidelines in their degree programs?

Based on our findings and teaching experience, we discuss the current state of cybersecurity education and summarize recommendations and best practices. We believe our work is beneficial for study program directors, coordinators, and educators who design and deliver the programs and courses.

1.4 Paper Outline

Section 2 summarizes previous related academic research. Section 3 details the methods used to select and analyze the offered study programs. Section 4 presents the findings and highlights examples of best practices. Section 5 offers a checklist for directors of current and prospective cybersecurity programs. Section 6 concludes the paper and provides recommendations for future improvements.

2 Prior and Related Work

Since our paper examines entire study programs, we review other publications of a similar type. This means we focus on papers that also deal with university programs or broader curricular issues (in Section 2.1), not papers about a single course or an isolated cybersecurity exercise. Section 2.2 follows up with a discussion of skills that cybersecurity graduates need for the job market.

2.1 Cybersecurity Study Programs

The most recent and related paper to ours is a review of cybersecurity education in the USA [11]. The authors analyzed descriptions of cybersecurity programs at 100 institutions – Centers of Academic Excellence (CAE) in Cybersecurity. They concluded that these institutions should ensure their curricula match the needs of industry, so that their graduates are work-ready specialists.

While Crabb et al. [11] focused on the USA, our analysis is global, including 68 institutions outside the USA. Finally, Crabb et al. [11] did not publish a dataset or supplementary materials providing details about the analyzed programs. As a result, we are unable to report the overlap in terms of which programs they analyzed are also included in our study. We can only report that our dataset contains 13 programs of the CAE-designated institutions.

Next, Blaine et al. [5] described the evolution of a cyber science study program at the US Military Academy. The study program aims at undergraduates and is consistent with various curricular guidelines, including CSEC2017 [31]. It consists of core foundational courses, such as programming and networking, and elective specializations, such as cybersecurity, cyber operations, or cyber-physical systems. Based on their experience, the authors provide recommendations to faculty members at other institutions that consider adding a new cyber major. For example, they suggest “an incremental approach [...] by progressively introducing electives to existing programs, such as [computer science]”.

Asghar and Luxton-Reilly [2] reflected on a cybersecurity master degree program in New Zealand. They mapped the content of the courses to a competency-based framework [23], demonstrating the coverage of adversarial aspects as well as interdisciplinary elements. Apart from describing the courses and graduate profiles, they also shared the experience with institutional requirements, such as quality assurance and program evaluation. Similarly to Blaine et al. [5], their experience may be valuable for educators who intend to establish a new degree program at their university.

da Veiga et al. [14] sought to create a cybersecurity curriculum for universities by examining the current best practices. They focused on their national context of South Africa, concluding that “South African universities do not have a formal undergraduate course in cybersecurity” (as of 2021). Therefore, they selected five high-ranked universities (three in Australia and two in the UK) with cybersecurity degree programs, and complemented their review with seven academic survey papers, resulting in 49 cybersecurity modules. The most commonly occurring ones featured skills regarding networks, cryptography, and forensics.

Overall, while the prior publications reviewed above examine relevant curricular initiatives, to the best of our knowledge, no paper provides a global perspective as broad as our analysis.

2.2 Cybersecurity Job Market

Graham and Lu [17] analyzed 17,929 online job advertisements for cybersecurity positions. Apart from the requirements on technical skills, which were often focused on data (data protection, loss prevention, and privacy), the job postings strongly emphasized non-technical skills, including communication, teamwork, and problem-solving. This is consistent with earlier work by Jones et al. [19] who interviewed 44 cyber professionals on the most important skills that cybersecurity students should learn in school. The technical skills included, for example, understanding how network traffic flows and how to harden operating systems. The non-technical skills included mainly communication, presentation skills, and collaboration.

In a related work, Özyurt and Ayaz [43] analyzed 9,407 cybersecurity job postings. The advertised job roles were divided into ten categories (e.g., engineer, analyst, or manager), with each category further subdivided into specific job titles. In addition, automated topic modeling identified 23 topic categories (e.g., security operations, risk management, and business/customer services) within the job postings. The mapping between the job roles and the topics revealed which types of skills are more relevant for which types of positions, highlighting the spectrum between more technically-oriented and more human/organization-oriented roles.

Generally, the analysis of the current job market proves the importance of both technical and non-technical competencies, as well as the value of hands-on skills. This is strongly aligned with the cybersecurity curricular guidelines that we use as a baseline.

3 Global Survey of Cyber Programs

In this paper, we seek to understand how the CSEC curricular guidelines [31], which were published in 2017, have been adopted in higher education. To achieve this goal, we review study programs from 101 universities and present our position through the subsequent data analysis. Figure 2 shows the overview of our approach.

The authors of this paper have extensive experience with cybersecurity education – both with teaching and publishing research in this field. Two co-authors are associate professors at a computer science department of a large university, which has a dedicated 3-year bachelor’s program in cybersecurity and 2-year master’s programs in information security and cybersecurity management. They have been teaching cybersecurity at a university level since 2015 and are interested in how it is taught worldwide. *The authors do not come from universities whose programs were examined.*

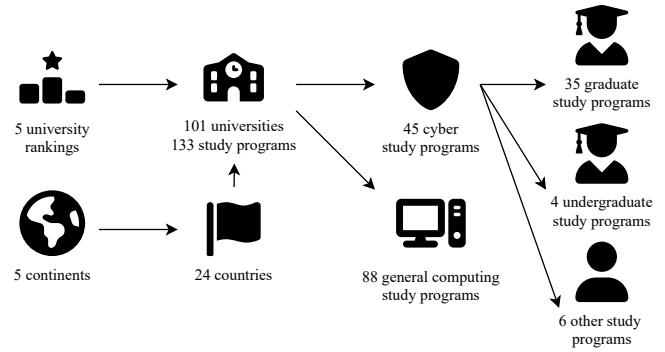


Figure 2: Overview of the explored study programs.

3.1 Selection of Universities

We surveyed top universities according to five different internationally recognized rankings (color-coded for readability in Table 1):

- (1) top 50 from Times Higher Education World University Rankings 2024 by the subject of computer science [36] (THE-WU),
- (2) top 50 from QS World University Rankings 2024 by the subject of computer science and information systems [26] (QS-WU),
- (3) top 50 from EduRank Best Universities for Cybersecurity 2024 in the World [16] (EDU),
- (4) top 31 universities from top 10 countries in Global Cybersecurity Index 2020 (GCI) capturing “the commitment of countries to cybersecurity at a global level” [37],
- (5) top 15 from Times Higher Education Emerging Economies University Rankings 2022 [35] (THE-EE).

The rationale behind this selection is an attempt to include not only the top universities in computer science, which are predominantly located in the USA, but also those focusing on cybersecurity and/or outside the USA. To complement the two traditional rankings (THE-WU and QS-WU), we use EDU, which relies only on metrics of research performance (OpenAlex citation database), non-academic prominence (backlinks on the Internet), and alumni score (page views at Wikipedia) [16]. We added the top 50 universities in the world and at least two highest-ranked universities in EDU from each country in the top 10 countries in the GCI except the USA (#1 in GCI)¹. Finally, to ensure truly global coverage, we searched for cybersecurity programs also at universities from emerging economies (THE-EE) that may be motivated to keep up with the developed countries and established universities.

3.2 Extraction of Study Programs’ Information

Two authors conducted the survey of study programs, with the first author double-checking and confirming the collected information to ensure its validity.

For each university, we searched their respective websites for any offered cybersecurity study programs, except Ph.D. (doctoral). If the said institution did not offer a program with the word “cyber” in its name, then we resorted to looking for their post-graduate degrees that are related to computer security/science. Examples of

¹If we had already added two universities from a country from GCI based on THE-WU or QS-WU, we added a third based on EDU. There were 14 countries ranked #2 to #10 in GCI; for three of them we added the third university, which resulted in 31 in total.

these include *Master in Information Security* or *Master in Informatics*. Undergraduate and associate degrees in computer science were not considered in the analysis. In sum, we tried to exhaust all computing-related post-graduate degrees to be included in our dataset as proof we did not omit to examine the offerings of a given institution.

For all programs having “cyber” in their name, we manually collected their type, duration, links to their curricula, and study or course catalogs (if available). Then, we inspected the catalogs and course descriptions to find out *i*) whether the core courses or core electives cover the CSEC2017 areas of human, organizational, and societal security (see Section 4.3); and *ii*) hands-on learning components (see Section 4.4), namely: requirements for completing internships (work placements); a semester/pre-capstone project, the final capstone project, or final thesis.

3.3 Limitations of the Survey Approach

There are two main limitations that could influence the findings. First, if a university or a country is not present in any of the rankings (THE-WU, QS-WU, EDU, GCI, or THE-EE), its cybersecurity program will not appear in our analysis, even though it may be of high quality. Second, if the website of the study program has not been updated recently by the university, the information may not fully reflect the latest status of the program.

4 Findings and Examples of Good Practice

This section summarizes the survey results and highlights good practices. The dataset with all collected information about the study programs and a Python notebook for its processing is available [40].

4.1 Composition of Discovered Programs

A total of 133 study programs at 101 universities from 24 countries (see Table 1) were enumerated. The Spearman correlation among THE-WU and EDU rankings of all universities is 0.68, $p < 0.001$. The correlation among QS-WU and EDU is 0.65, $p < 0.001$. This means that universities generally higher in THE-WU or QS-WU do not necessarily merit a similar ranking in EDU, supporting our decision to include multiple rankings in the analysis.

The 101 universities offer only 45 programs with “cyber” in its name. The most prevalent are graduate (35), mostly master’s. The rest are undergraduate (4) and other (6), such as post-baccalaureate or graduate certificates. The graduate programs typically last from 1 to 2 years, the undergraduate from 3 to 5.5 years, and others a few months. Most cyber programs overall are offered in the USA (17). Elsewhere, a maximum of three cybersecurity programs is offered.

The remaining 88 non-cyber programs include general computing programs, such as computer science, computer engineering, or software engineering. Some programs allow studying security or cybersecurity track or concentration. A few universities offer an information security program.

From this point on, we will only focus on discussing the 45 cyber programs, since they best reflect the topic of this paper.

4.2 Slow Adoption of Guidelines and Trends

The data indicates that the top-ranked universities have not widely adopted the existing curricular guidelines. Even though cybersecurity is a distinct computing discipline, and there are specialized

Table 1: Breakdown of 101 examined institutions per country.

Country	Institutions	Source ranking(s)
USA	33	THE-WU, QS-WU, EDU
China (Mainland)	12	THE-WU, QS-WU, EDU, THE-EE
United Kingdom	6	THE-WU, QS-WU, EDU, GCI
Canada	5	THE-WU, QS-WU, GCI
France	4	THE-WU, QS-WU, GCI
Russian Federation	4	GCI, THE-EE
Australia	3	QS-WU, EDU
China (Hong Kong)	3	THE-WU, QS-WU, EDU
Korea (Rep. of)	3	THE-WU, QS-WU, GCI
Estonia	2	GCI
Germany	2	THE-WU, QS-WU
India	2	GCI
Japan	2	THE-WU, QS-WU, GCI
Lithuania	2	GCI
Malaysia	2	GCI
Netherlands	2	THE-WU, QS-WU
Saudi Arabia	2	GCI, THE-EE
Singapore	2	GCI
Spain	2	GCI
Switzerland	2	THE-WU, QS-WU, EDU
United Arab Emirates	2	GCI
Belgium	1	THE-WU, EDU
Italy	1	QS-WU
South Africa	1	THE-EE
Taiwan	1	THE-EE
Total	101	

cybersecurity curricular frameworks (such as CSEC2017), many top universities do not provide any cybersecurity program, or offer only a certificate after passing a few semester-long courses.

Next, the majority of cyber programs do not relate themselves to the existing systematization initiatives, such as NSA CAE in Cybersecurity for curriculum and program requirements, or NIST NICE framework for describing cybersecurity tasks, knowledge, and skills. In particular, only 6 out of 17 cyber programs offered in the USA have been validated by NSA. However, the total number of NSA-designated institutions was 444 as of July 1, 2024 [7]. A good example of using external frameworks is the website of master program *Cybersecurity* at New York University [21], which presents the requirements for completing Cyber Defense and Cyber Operations tracks defined by NSA CAE in Cybersecurity.

There is also room for developing undergraduate programs. Our survey identified only four bachelor programs at top-ranked universities. However, three- or four-year-long programs enable more focus and specialization in cybersecurity than general computing programs or shorter master programs and certificates. The longer programs could also include more experiential learning, such as industry internships. A good example is the 4-year bachelor program in *Cybersecurity Analytics and Operations* at Pennsylvania State University [24]. This program contains dedicated cybersecurity courses, such as Cyber Incident Handling and Response, Cyber-Defense Studio, Malware Analytics, mandatory internship, and a cybersecurity capstone project. There are other educational institutions that may provide this value through bachelor’s programs – in the USA alone, there are 178 programs available [12] – but often offered by other than top-ranked universities. Thus, they were not reflected in this survey due to the choice of the university rankings.

4.3 Inclusion of Non-technical Areas of Security

CSEC2017 curriculum guidelines recognize eight Knowledge Areas (KAs), which serve as the basic organizing structure for cybersecurity topics [31]. Further, the guidelines list the essential concepts in all KAs that comprise the minimum required content for any cybersecurity program. In reference to these guidelines, Blažič [6] argued that one of the ways to fulfill the demand for qualified professionals (cybersecurity skills gap) is the enrichment of the curricula with new content from the KAs that are covered the least, such as the organizational or human aspects of cybersecurity.

Therefore, we analyzed program websites and publicly available online materials to find out how the non-technical areas are represented. Namely, we searched for essential concepts defined in CSEC2017 for *human, organizational, and societal security* in the descriptions of core or core elective courses. If the concepts were only one or two topics out of ten or more in a single, typically introductory course, we did not count it. Most often (25×), the courses cover topics of organizational security, such as risk management, governance and policy, incident management, or security operations. Less often (12×), they include societal security topics, for instance, cyber crime, cyber law, and cyber ethics. The least represented (6×) were topics of human security, for example, identity management, social engineering, or personal data privacy and security.

Only five programs cover topics in the three KAs. One of these programs is a joint 2-year master *Cybersecurity* at Estonian universities, Tallinn University of Technology and University of Tartu [29]. This program requires passing several semester-long courses dealing with the non-technical areas, such as Human Aspects of Cyber Security, Legal Aspects of Cyber Security, and Cyber Security Management. It also offers core electives, such as Privacy-preserving Technologies, Strategic Communications and Cybersecurity, Cyber Incident Handling, or Intelligence Methods for Cyber Professionals.

We believe that one of the reasons for the overall unsatisfactory situation is the lack of time in the master programs and the subsequent prioritization of technical KAs, such as data security, connection security, or system security. To address this gap, program directors at universities with faculties of law or social studies can consider enhancing their cybersecurity programs with relevant courses from these faculties. However, our experience from teaching at a university that offers a program with such courses shows that the course content needs to be adapted to be relevant to computing students and their future careers.

4.4 Hands-on and Experiential Learning

CC2020 argues that *competency* (as opposed to just knowledge) should be the standard for describing computing curricula. This can involve “stronger focus on various forms of experiential learning, from interactive simulations, to intensive projects, to field experiences, and to internships and cooperative programs with industry” [8]. However, to fulfill this requirement, “domain-specific skills and dispositions require a learning environment that is different from a traditional classroom environment” [8]. Accordingly, we examined whether the programs require completing internships in workplace-relevant settings and creating a final or capstone project or thesis that involves independent student work.

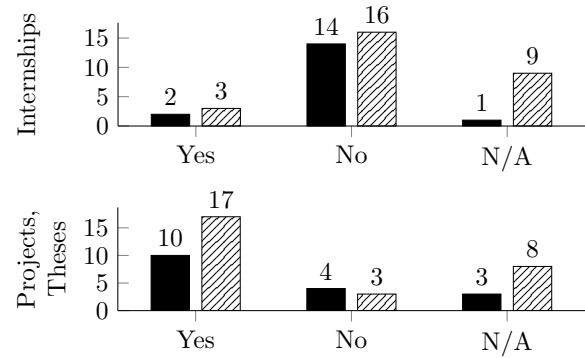


Figure 3: Internships and final projects/theses for 17 US programs (black) and 28 outside the USA (hatch fill). “N/A” means the program descriptions do not contain this information.

4.4.1 Internships. Figure 3 shows how many programs from the USA and outside require an internship. The mandatory internships are present only in five programs (11%). A notable example is bachelor *Cybersecurity Engineering* at Tallinn University of Technology, which allocates a considerable number of credits (24 out of 180 ECTS credits) to the application of the gained skills and competencies in an authentic field-related working environment [28].

However, including internships in a program assumes that all students will have enough opportunities to find a work placement that will be beneficial to their learning. This assumption might be difficult to fulfill for programs that have many students in regions with less-developed IT and cybersecurity ecosystems. Another challenge is the internship administration and assessment.

4.4.2 Projects and Theses. The distribution of programs from the USA and outside that require a final project/thesis is shown in Figure 3. The final project/thesis is mandated by 27 programs (60%). The projects typically require independent student’s work supervised by a faculty advisor on a cybersecurity topic. There are also projects where students interact with various organizations from a public, private, or nonprofit sector, solve their cybersecurity issues, and propose possible solutions. Three programs include a mandatory semester-long or pre-capstone project. Completing both internship and final project/thesis is required by only four programs (9%).

Regarding the written final thesis, we second to Perkins et al. [25] who advocates for reducing the reliance on assessments where AI tools may be used to mimic human writing. Following the CC2020 recommendations, we suggest instead requiring the completion of an intensive practical project. However, projects bring other challenges, such as creating meaningful and workplace-relevant assignments and assessment of artifacts created by students.

5 Cybersecurity Program Director’s Checklist

Based on the study findings and our experience, we created a 10-item checklist for directors of existing or prospective cybersecurity programs to initiate and support enhancements in their programs.

- (1) Is your *program different* enough from other computing programs offered at your university?

A dedicated cybersecurity program should include unique

core courses not offered in other computing programs, ensuring specialized training for students.

- (2) Does your program cover *all knowledge areas* defined by CSEC2017 [31]? Do you cover non-technical areas, such as *legal and privacy aspects*?

Since cybersecurity is an interdisciplinary field [31], consider involving specialists from non-computing areas, such as from other faculties or external experts. Subsequently, ensure their courses match the expected proficiency of the students.

- (3) Does your program teach *specifics of national or regional regulations and laws*?

Even though cyberspace is global, nations regulate it differently [1]. Your graduates will benefit from courses covering the regulations relevant to their country or region. For instance, universities in the EU countries may teach directives valid for member countries and their local law [32].

- (4) Have you switched from the knowledge-based to the *competency-based description of the curriculum* as suggested by CC2020 [8]?

Using *competencies* instead of knowledge may encourage adopting new forms of experiential learning, as discussed in Section 4.4. This can be a vital step to beat the skills gap [11].

- (5) How can you *include internships*?

Since internships must be centered around cybersecurity, consider the appropriate credit allocation. Also, consider whether the surrounding cybersecurity ecosystem in your city or area can accommodate your students and still provide them with relevant mentoring and topics.

- (6) Do you offer several *cybersecurity elective courses*?

This enables students to specialize in a cybersecurity area of their choice. Such specialization would be valued by their future employers seeking that specific expertise [17, 19, 43].

- (7) Does your school have *sufficient lab environment* to teach hands-on courses?

The practical activities often do not scale well, particularly in physical computer labs. Online training platforms [4] can address this issue with the benefit of being available to your students when needed. However, be aware that hands-on classes come with the cost of more laborious preparation and delivery on the instructors' side compared to onsite or online lectures and demonstrations.

- (8) Does your school have access to up-to-date *training materials and environments* for hands-on classes? Can your instructors create and maintain these materials independently?

Relevant teaching content that involves practice is key for programs that aim to fill the cybersecurity skills gap [11]. Reusing and sharing training materials is challenging because classes are highly dependent on the technical environment. Still, instructors can leverage existing resources such as the CLARK Cybersecurity Library [13].

- (9) Have you considered *changing the assessment* of courses, final projects, and thesis, given the spread of AI tools [25]?

We believe that AI tools should be allowed in class and during assessments (exams, mid-term tests, and final projects)

because practitioners use them as well. However, the assessments should move from simple question-and-answer formats to more complex assignments testing whether students can use concepts, tools, infrastructures, and data to produce useful output, thereby mimicking authentic workplace tasks [22].

- (10) Do you *use existing national or international frameworks* when designing or describing the program or its courses?

These frameworks can serve as a common language across different worlds of universities, students, employers, and governments. For examples, see the list in Section 1.1.

6 Conclusion

To answer the question posed in this paper's title, we examined how top-ranked world universities responded to the existing curricular guidelines (CSEC2017 and CC2020), which consider cybersecurity as a distinctive and interdisciplinary field. Among 101 higher education institutions analyzed, we identified only 45 cybersecurity programs. It is concerning that out of these 45, only five cover all eight knowledge areas defined by CSEC2017, especially organization, societal, and human security. Other programs cover only areas traditionally taught in computer science or engineering programs or their security concentrations, such as data or system security. Next, internships that enable practicing competencies and dispositions as promoted by CC2020 are mandated only by five programs. While more than half of the programs require a final project or thesis, six programs require neither an internship nor a final project/thesis. This lack of hands-on experience may leave graduates underprepared for their future careers. To support our claims, the dataset we collected is available as a supplementary material [40].

6.1 Recommendations for Future Improvements

Our analysis revealed a fragmentation of information about study programs and courses. First, there is no global ranking specifically for universities that offer cybersecurity programs. The well-known QS World University Rankings or Times Higher Education World University Rankings do not recognize cybersecurity as a distinctive subject (as opposed to computer science, and most recently data science and AI). EduRank considers only research metrics, excluding teaching. As a result, prospective students and program directors cannot easily find and compare available program offerings. Moreover, the study program directors cannot use such rankings as a benchmark to initiate and foster improvements in their programs.

Further, descriptions of the program structure, content, and requirements are presented mostly in general language, with no reference to existing frameworks, such as CSEC2017 knowledge areas; NICE work roles, tasks, knowledge, and skills; or NSA CAE knowledge units. This is another barrier to comparing individual programs for both students and directors. Instead, universities could better leverage these frameworks to enable program comparison. Lastly, governments and higher education analytics companies could compile rankings focusing solely on cybersecurity programs.

Acknowledgments

This research has received funding from the European Union's Horizon Europe program under Grant Agreement No. 101087529.

References

- [1] Saleh AlDaajeh, Heba Saleous, Saed Alrabaa, Ezedin Barka, Frank Breiteringer, and Kim-Kwang Raymond Choo. 2022. The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security* 119 (2022), 102754. <https://doi.org/10.1016/j.cose.2022.102754>
- [2] Muhammad Rizwan Asghar and Andrew Luxton-Reilly. 2020. A Case Study of a Cybersecurity Programme: Curriculum Design, Resource Management, and Reflections. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (Portland, OR, USA) (SIGCSE '20). ACM, New York, NY, USA, 16–22. <https://doi.org/10.1145/3328778.3366918>
- [3] William F. Atchison, Samuel D. Conte, John W. Hamblen, Thomas E. Hull, Thomas A. Keenan, William B. Kehl, Edward J. McCluskey, Silvio O. Navarro, Werner C. Rheinboldt, Earl J. Schweppe, William Viavant, and David M. Young. 1968. Curriculum 68: Recommendations for Academic Programs in Computer Science: A Report of the ACM Curriculum Committee on Computer Science. *Commun. ACM* 11, 3 (March 1968), 151–197. <https://doi.org/10.1145/362929.362976>
- [4] Razvan Beuran, Jan Vykopál, Daniela Belajová, Pavel Čeleda, Yasuo Tan, and Yoichi Shinoda. 2023. Capability Assessment Methodology and Comparative Analysis of Cybersecurity Training Platforms. *Computers & Security* 128 (2023), 103120. <https://doi.org/10.1016/j.cose.2023.103120>
- [5] Raymond W. Blaine, Jean R. S. Blair, Christa M. Chewing, Rob Harrison, James J. Raftery, and Edward Sobieski. 2021. Creating a Multifarious Cyber Science Major. In *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education* (Virtual Event, USA) (SIGCSE '21). ACM, New York, NY, USA, 1205–1211. <https://doi.org/10.1145/3408877.3432462>
- [6] Borka Jerman Blažič. 2022. Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Education and information technologies* 27, 3 (2022), 3011–3036. <https://doi.org/10.1007/s10639-021-10704-y>
- [7] CAE in Cybersecurity Community. 2024. CAE Institution Map. Online, accessed July 8, 2024, map last updated July 1, 2024. <https://www.caecommunity.org/cae-map>
- [8] CC2020 Task Force. 2020. *Computing Curricula 2020: Paradigms for Global Computing Education*. ACM, New York, NY, USA. <https://doi.org/10.1145/3467967>
- [9] Shuai Chen, Mengmeng Hao, Fangyu Ding, Dong Jiang, Jiping Dong, Shize Zhang, Qiquan Guo, and Chundong Gao. 2023. Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications* 10, 1 (23 Feb 2023), 71. <https://doi.org/10.1057/s41599-023-01560-x>
- [10] Wm. Arthur Conklin, Raymond E. Cline, and Tiffany Roosa. 2014. Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. In *2014 47th Hawaii International Conference on System Sciences*. IEEE, New York, NY, USA, 2006–2014. <https://doi.org/10.1109/HICSS.2014.254>
- [11] James Crabb, Christopher Hundhausen, and Assefaw Gebremedhin. 2024. A Critical Review of Cybersecurity Education in the United States. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education* (SIGCSE 2024). ACM, New York, NY, USA, 241–247. <https://doi.org/10.1145/3626252.3630757>
- [12] Cybersecurity Guide Contributors. 2024. Cybersecurity Guide. <https://cybersecurityguide.org/programs/cybersecurity-bachelors-degree/#Schools> Online, last updated: May 10, 2024.
- [13] Cybersecurity Library. 2024. CLARK. Online, accessed July 15, 2024. <https://clark.center/home>
- [14] Adèle da Veiga, Elisha Ochola, Mathias Mujinga, Keshnee Padayachee, Emilia Mwim, Elmarie Kritzing, Marianne Looock, and Peeha Machaka. 2021. A Reference Point for Designing a Cybersecurity Curriculum for Universities. In *Human Aspects of Information Security and Assurance*, Steven Furnell and Nathan Clarke (Eds.). Springer International Publishing, Cham, 46–62. https://doi.org/10.1007/978-3-030-81111-2_5
- [15] P. J. Denning, D. E. Comer, D. Gries, M. C. Mulder, A. Tucker, A. J. Turner, and P. R. Young. 1989. Computing as a discipline. *Computer* 22, 2 (1989), 63–70. <https://doi.org/10.1109/2.19833>
- [16] EduRank.org. 2024. Best Universities for Cyber Security in the World [updated February 29, 2024]. Online, accessed June 18, 2024. <https://edurank.org/cs/cybersecurity/>
- [17] C. Matt Graham and Yonggang Lu. 2023. Skills Expectations in Cybersecurity: Semantic Network Analysis of Job Advertisements. *Journal of Computer Information Systems* 63, 4 (2023), 937–949. <https://doi.org/10.1080/08874417.2022.2115954>
- [18] Mark Guzdial. 2018. What We Care about Now, What We'll Care about in the Future. *ACM Inroads* 9, 4 (Nov. 2018), 63–64. <https://doi.org/10.1145/3276304>
- [19] Keith S. Jones, Akbar Siami Namin, and Miriam E. Armstrong. 2018. The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals. *ACM Trans. Comput. Educ.* 18, 3 (2018), 12 pages. <https://doi.org/10.1145/3152893>
- [20] Džedjiga Mouheb, Sohail Abbas, and Madjid Merabti. 2019. Cybersecurity Curriculum Design: A Survey. In *Transactions on Edutainment XV*. Springer, Berlin, Heidelberg, 93–107. https://doi.org/10.1007/978-3-662-59351-6_9
- [21] New York University, Tandon School of Engineering. 2024. Cybersecurity (MS). Online, accessed July 11, 2024. <https://bulletins.nyu.edu/graduate/engineering/programs/cybersecurity-ms/>
- [22] Marc Ohm, Christian Bungartz, Felix Boes, and Michael Meier. 2024. Assessing the Impact of Large Language Models on Cybersecurity Education: A Study of ChatGPT's Influence on Student Performance. In *Proceedings of the 19th International Conference on Availability, Reliability and Security* (Vienna, Austria) (ARES '24). Association for Computing Machinery, New York, NY, USA, Article 104, 7 pages. <https://doi.org/10.1145/3664476.3670446>
- [23] Allen Parrish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou. 2018. Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-discipline. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (Larnaca, Cyprus) (ITICSE '18). ACM, New York, NY, USA, 36–54. <https://doi.org/10.1145/3293881.3295778>
- [24] Pennsylvania State University. 2024. Cybersecurity Analytics and Operations, B.S. Online, accessed July 11, 2024. <https://bulletins.psu.edu/undergraduate/colleges/information-sciences-technology/cybersecurity-analytics-operations-bs/>
- [25] Mike Perkins, Jasper Roe, Darius Postma, James McGaughan, and Don Hickerson. 2024. Detection of GPT-4 Generated Text in Higher Education: Combining Academic Judgement and Software to Identify Generative AI Tool Misuse. *Journal of Academic Ethics* 22, 1 (2024), 89–113. <https://doi.org/10.1007/s10805-023-09492-6>
- [26] Quacquarelli Symonds. 2024. QS World University Rankings by Subject: Computer Science and Information Systems 2024. Online, accessed June 18, 2024. <https://www.qschina.cn/en/university-rankings/university-subject-rankings/2024/computer-science-and-information-systems>
- [27] Ying Sui. 2024. The Investigation of Cybersecurity Education Among College Students: Aiming to Address the Scarcity of Skilled Professionals. *The Educational Review*, USA 8, 6 (2024), 801–807. <https://www.proquest.com/scholarly-journals/investigation-cybersecurity-education-among/docview/3084053340/se-2>
- [28] Tallinn University of Technology. 2024. Cyber Security Engineering. Online, accessed July 12, 2024. <https://ois2.taltech.ee/usoisois/programme/IVSB17/23>
- [29] Tallinn University of Technology. 2024. Cybersecurity. Online, accessed July 12, 2024. <https://ois2.taltech.ee/usoisois/programme/IVCM09/24>
- [30] The ACM Committee for Computing Education in Community Colleges (CCECC). 2020. Cybersecurity Curricular Guidance for Associate-Degree Programs. Online, accessed May 27, 2024. <https://cecc.acm.org/guidance/cybersecurity>
- [31] The ACM Joint Task Force (JTF) on Cybersecurity Education. 2017. Cybersecurity Curricular Guideline. Online, accessed May 27, 2024. <http://cybered.acm.org>
- [32] The European Union Agency for Cybersecurity (ENISA). 2022. European Cybersecurity Skills Framework (ECSF). Online, accessed May 27, 2024. <https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework>
- [33] The National Cyber Security Centre (NCSC). 2021. The Cyber Security Body Of Knowledge (CyBOK) v. 1.1. Online, accessed May 27, 2024. <https://www.cybok.org/>
- [34] The National Institute of Standards and Technology (NIST). 2020. National Initiative for Cybersecurity Education (NICE). Online, accessed May 27, 2024. <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center>
- [35] Times Higher Education. 2021. Emerging Economies University Rankings 2022. Online, accessed June 18, 2024. <https://www.timeshighereducation.com/world-university-rankings/2022/emerging-economies-university-rankings>
- [36] Times Higher Education. 2023. World University Rankings 2024 by subject: computer science. Online, accessed June 18, 2024. <https://www.timeshighereducation.com/world-university-rankings/2024/subject-ranking/computer-science>
- [37] International Telecommunication Union. 2020. Global Cybersecurity Index. Online, accessed June 18, 2024. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>
- [38] Valdemar Švábenský. 2022. *Automated Feedback for Cybersecurity Training*. Doctoral thesis. Masaryk University. <https://is.muni.cz/th/dg3b4/?lang=en>
- [39] Valdemar Švábenský, Jan Vykopál, and Pavel Čeleda. 2020. What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITICSE Conferences. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (Portland, OR, USA) (SIGCSE '20). ACM, New York, NY, USA, 2–8. <https://doi.org/10.1145/3328778.3366816>
- [40] Jan Vykopál, Valdemar Švábenský, Michael T. Lopez II, and Pavel Čeleda. 2024. Dataset: Cybersecurity Study Programs. Online, accessed November 8, 2024. <https://gitlab.fi.muni.cz/cybersec/papers/2025-sigcse-cybersecurity-programs>
- [41] Richard Weiss, Jens Mache, Elizabeth Hawthorne, Ambareen Siraj, Blair Taylor, Siddharth Kaza, and Ankur Chattopadhyay. 2021. Integrating Hands-on Cybersecurity Exercises into the Curriculum in 2021. In *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education* (Virtual Event, USA) (SIGCSE '21). ACM, New York, NY, USA, 1358. <https://doi.org/10.1145/3408877.3439530>
- [42] Sherri Weid-Harms, Adam Spanier, John Hastings, and Matthew Rokusek. 2023. A Systematic Mapping Study on Gamification Applications for Undergraduate Cybersecurity Education. *Journal of Cybersecurity Education, Research and Practice* 2023, 1 (2023), 9. <https://doi.org/10.32727/8.2023.12>
- [43] Özcan Özyurt and Ahmet Ayaz. 2024. Identifying cyber security competencies and skills from online job advertisements through topic modeling. *Security Journal* – (2024), 21 pages. <https://doi.org/10.1057/s41284-024-00420-w>